

# PLANNING FOR EMERGENCIES

## SIX BASIC ELEMENTS OF A VULNERABILITY ASSESSMENT

- 1) Name and describe the system facilities, treatment processes, operating procedures and mission objectives.
- 2) Starting with the worst case, identify what can go wrong with the system and what the results would be.
- 3) Identify hostile actions or harmful events that could cause serious problems.
- 4) Assess how likely such hostile actions or harmful events could occur.
- 5) Evaluate existing protection measures.
- 6) Develop a plan to lower the risk of such events starting with the worst possible event.

## EMERGENCY RESPONSE PLANNING—Identify:

- Who will do what
- When it should be done
- With what resources it will be done
- By what authorities or persons it will be done

## SECURITY PLAN OUTLINE

- **The Introduction:** reason for the plan
- **Vulnerability Assessment Results:** lists and details the vulnerability assessment findings
- **Upgrade Plan:** the duties and goals required, with the time and costs needed to do them
- **Roles and Responsibilities:** who does what to establish and manage security
- **Policy & Procedure Development:** policies and procedures for access control, barriers, delays, intrusion detection, testing and maintenance
- **Emergency and Contingency Measures:** activities for specific emergency conditions—how to deal with bomb and contamination threats, chemical spills and releases, injured staff, sabotage, destruction of equipment, etc.

## EIGHT CORE ELEMENTS OF AN EMERGENCY RESPONSE PLAN (ERP)

1. System Specific Information
2. Personnel Roles and Responsibilities
3. Communication Procedures: Who, What and When
4. Personnel Safety
5. Identification of Alternate Water Sources
6. Replacement Equipment and Chemical Supplies
7. Property Protection
8. Water Sampling and Monitoring

## BUSINESS CONTINUITY PLANNING

Planning to limit risk and to maintain investments, operating procedures, staff levels and duties, ones of communication and other activities to ensure:

READINESS: preparation for disasters and extreme events.

RESPONSE: how to cope with disasters and extreme events.

RECOVERY: restoring normal operations after completing the response.